VMware vCenter Log Insight User's Guide

vCenter Log Insight 1.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001131-00

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About VMware vCenter Log Insight User's Guide

The *VMware vCenter Log Insight User's Guide* provides information about using the web user interface of VMware® vCenter™ Log Insight™, including how to filter and search log messages, perform analysis on the search results, and dynamically extract fields from log messages based on customized queries.

Intended Audience

This information is intended for anyone who wants to use Log Insight.

Using Log Insight 1

Log Insight provides scalable log aggregation and indexing for the vCloud Suite, including base editions of vSphere, with near real-time search and analytics capabilities.

Log Insight collects, imports, and analyzes logs to provide real-time answers to problems, and derive important insights about systems, services, and applications.

High Performance Ingestion

Log Insight can process any type of log or machine generated data. Log Insight supports very high throughput rates and low latency. The data is available for search and analysis within a few seconds from the moment they arrive to Log Insight. Log Insight accepts data through syslog.

Near Real-Time Search

From the moment the data arrives to Log Insight, it is available for search within seconds. Also, historical data can be searched from the same interface with the same low latency.

Log Insight supports wildcard searching (for example, erro?, vm*) and field based filtering (for example, hostname does NOT match test*, IP contains "10.64"). Furthermore, fields that contain numeric values can be used to define selection constraints (for example, CPU>80, 10<threads<100, and so on).

Search results are presented as a single continuous log even if they come from multiple sources. You can use Log Insight to correlate the data on one or multiple dimensions (for example, time and request identifiers) providing a coherent view across the stack. This way, root cause analysis becomes much easier.

Aggregation

Fields that are extracted from log data can be used for aggregation. This is similar to the functionality that GROUP-BY queries provide in a relational database or pivot-tables in Microsoft Excel. The difference is that there is no need for ETL, and Log Insight scales to any size of data.

You can generate aggregate views of the data and identify specific events or errors without having to jump between systems and applications. For example, while viewing an important system metric, for example, number of errors per minute, you can drill down to a specific time-range of events and examine the errors.

Runtime Field Extraction

Raw log data is not always easy for you to understand, and it takes some data processing to identify the fields that are important for searching and aggregation. Log Insight provides runtime field extraction to address this problem. You can dynamically extract any field from the data by providing a regular expression. The extracted fields can be used for selection, projection, and aggregation, similar to how the fields that are extracted at parse time are used.

Dashboards

You can create dashboards of useful metrics that you want to monitor closely. Any query can be turned into a dashboard widget and visualized for any range in time. You can check the performance of your system for the last hour, day, or week. You can view a break down of errors by hour and observe the trends in log events.

Security Considerations

IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of Log Insight must visit the VMware vCenter Log Insight documentation page and search for the latest version of the *VMware vCenter Log Insight Security Guide*.

The Security Guide contains concise reference to the security features of Log Insight. Topics include the product external interfaces, ports, authentication mechanisms, and options for configuration and management of security features.

This chapter includes the following topics:

Information in Log Events

You can import logs in Log Insight by using syslog. After the import, logs are split into individual events, or messages.

Each event contains the following information.

Type	Description
Timestamp	The time when the event occurred
Text	The raw text of the event
Source	Whether the event came from an ESXi host or a particular log file
Fields	A name-value pair extracted from the event

Overview of the Log Insight Web User Interface

The functionality that you can access depends on the user account that you use to log in to the Log Insight Web user interface.

The Dashboards Tab

The **Dashboards** tab contains custom dashboards and content pack dashboards. On the **Dashboards** tab, you can view graphs of log events in your environment, or create your custom sets of widgets to access the information that matters most to you.

The Interactive Analytics Tab

On the **Interactive Analytics** tab, you can search and filter log events, and create queries to extract events based on timestamp, text, source, and fields in log events. Log Insight presents charts of the query results. You can save these charts to look them up later on the **Dashboards** tab.

Content Packs

Content packs contain dashboards, extracted fields, saved queries, and alerts that are related to a specific product or set of logs. You access the content packs from the drop-down menu at the upper right of the Log Insight Web user interface.

Content packs can be imported or created by Log Insight users. See "Working with Content Packs," on page 11.

The Administration User Interface

Log Insight administrators can manage user accounts, configure storage location and archiving, configure an outgoing SMTP server for email notifications, and change several other parameters. The URL format of the Administration UI is https://*log_insight-host*/admin/, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Creating Dashboards Charts

You can view a predefined dashboard charts or create custom dashboard charts.

The default dashboard charts that are included in Log Insight are split into categories for custom dashboards and content pack dashboards.

Custom Dashboards

Custom dashboards are created by users of the current instance of Log Insight. Custom dashboards are organized in two groups, my dashboards and shared dashboards. My dashboards are visible only to the currently logged in user . Shared dashboards are visible to all users of Log Insight.

You can use the drop-down menu in the upper left corner of the **Dashboards** tab to switch between dashboard groups.

You can create new dashboards in My Dashboards or Shared Dashboards, depending on whether you want other people to access these new dashboards.

You can create, clone, rename, and delete custom dashboards.

You can create, clone, rename, delete, move, and resize log chart widgets in all custom dashboards.

Content Pack Dashboards

Content pack dashboards are imported with content packs.

NOTE Content pack dashboards are read-only. You cannot delete or rename them. However, you can clone content pack dashboards to your custom dashboard. You can clone whole dashboards or individual widgets.

Managing Dashboards and Log Charts

You can create and delete log chart widgets and custom dashboards in Log Insight.

IMPORTANT Log Insight does not perform checks for duplicate names of the dashboards, queries, and alerts that you save or clone. The display name is not an unique identifier when saving queries in Log Insight. Therefore, you can save multiple charts, alerts, and dashboards with the same name. To ease data retrievability, do not duplicate names when you save charts, alerts, or dashboards.

Custom dashboards are collections of queries and charts that you or other users save in Log Insight. Content pack dashboards and log chart widget cannot be modified, but you can clone those dashboards to your custom dashboards.

Table 1-1. Working with Custom Dashboards

Task	Procedure
Create a new custom dashboard	On the **Dashboards** tab, click **New Dashboard** in the lower left.
Edit the name of a custom dashboard	On the **Dashboards** tab, point to the dashboard name and select **Rename** from the drop-down menu.
Delete a custom dashboard	On the **Dashboards** tab, point to the dashboard name and select **Delete** from the drop-down menu.
Clone a dashboard from a content pack to your custom dashboard.	1 On the **Dashboards** tab, select a content pack and point to the dashboard that you want to clone. 2 Click the **Add to custom dashboards** icon. 3 Type a name and click **Save**.

Log charts represent graphical analysis of the log events for the specified time range.

Table 1-2. Working with Log Charts

Task	Procedure
Save a chart to your custom dashboard	1 At the upper left of the **Interactive Analytics** tab, click **Add to Dashboard**. 2 Type a name, select the destination dashboard from the drop-down menu, and click **Add**.
Change the time range of a chart	On the **Interactive Analytics** tab, use the **Time Range** drop-down menu to switch the period displayed in the chart.
Change the granularity of a chart	On the **Interactive Analytics** tab, use the buttons at the upper right to switch between 1 hour, 1 minute, and 5 seconds granularity of the chart.

Table 1-2. Working with Log Charts (Continued)

Task	Procedure
Load a chart on the **Interactive Analytics** tab	On the **Dashboards** tab, point to a query and click the **View in Interactive Analytics** icon. The time range is set to the current time range of the dashboard.
Delete a chart from your custom dashboard	1 On the **Dashboards** tab, select the custom dashboard that contains the graph that you want to delete. 2 In the upper right corner of the graph widget, click the actions icon ⚙, and select **Delete**. 3 In the Delete Widget dialog box, click **Delete** to confirm.

Working with Content Packs

Content packs contain dashboards, extracted fields, saved queries, and alerts that are related to a specific product or set of logs.

To view the content packs that are loaded on your system, select **Content Packs** from the drop-down menu in the upper right corner of the Log Insight user interface.

To view the contents of a content pack, click the content pack in the list on the left.

Custom Content

The Custom Content category contains dashboards, extracted fields, and queries created in the current instance of Log Insight. Custom content packs are organized in two groups, My Content and Shared Content. The My Content section contains the personal content of the currently logged in user. The Shared Content section contains content that is shared among all users of Log Insight .

Content Packs

The Content Packs category contains imported sets of dashboards, extracted fields, and queries.

NOTE Content pack dashboards are read-only. You cannot delete or rename them. However, you can clone content pack dashboards to your custom dashboard. You can clone whole dashboards or individual widgets.

Export a Content Pack

You can export your custom dashboards, saved queries, and extracted fields as a content pack.

Content packs are saved as vCenter Log Insight Content Pack (VLCP) files.

Prerequisites

- Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.
- Verify that you have personal custom content saved on the Content Manager page.

Procedure

1 From the drop-down menu on the upper right, select **Content Packs**.

2 On the Content Manager page, click the content that you want to export and select **Export Content Pack** from the drop-down menu at the end of the row.

3 Type a name for your content pack and click **Save**.

4 Browse to the location where you want to save the file and click **Save**.

The exported VLCP file appears in the location you selected.

Import a Content Pack in Log Insight

You can import content packs to exchange user-defined information with other instances of Log Insight, or to upgrade your old content packs with newer versions.

You can import only vCenter Log Insight Content Pack (VLCP) files.

Prerequisites

- Verify that your browser supports HTML5.
- Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 From the drop-down menu on the upper right, select **Content Packs**.

2 In the lower left corner, click **Import Content Pack**.

3 Browse for the content pack that you want to import, click **Open**, and click **Import**.

The imported content appears in the Content Packs list to the left.

NOTE Content pack dashboards are read-only. You cannot delete or rename them. However, you can clone content pack dashboards to your custom dashboard. You can clone whole dashboards or individual widgets.

Searching and Filtering Log Events

You can search and filter log events on the **Interactive Analytics** tab.

You can type any text in the search text box and click **Search** to find only events that contain this text.

Time ranges are inclusive when filtering.

You can search for log events that match certain values of specific fields.

You can specify the field search criteria, or constraint, by using the drop-down menus and the text box above the list of log events.

Within a single-row constraint, you can use comma-separated values to list OR constraints. For example, select **hostname equals** and type `127.0.0.1, 127.0.0.2`. The search returns events with the host name 127.0.0.1 or 127.0.0.2.

You can combine multiple field constraints by creating a new constraint row for each field. You can toggle the operator that is applied on multiple-row constraints .

- Select **all** to apply the AND operator.

- Select **any** to apply the OR operator.

NOTE Regardless of the toggle value, the operator for comma-separated values within a single constraint row is always OR.

You can use wildcards in search terms. For example, vm* or vmw?re.

- Use * for 0 or more characters
- Use ? for one character.

NOTE Wildcards cannot be used as the first character of a search term. For example, you can use 192.168.0.*, but you cannot use *.168.0.0 in your filtering queries.

Filter Log Events by Time Range

You can filter log events to view only the events for a certain period.

Time ranges are inclusive when filtering.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1. From the **Time Range** drop-down menu on the right, select one of the predefined periods.
2. (Optional) To set the initial and final point of the time range, select **Custom**.

Filter Log Events by Field Values

You can use the list of extracted fields to filter log events with specific values for a field.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1. Navigate to the **Interactive Analytics** tab.
2. In the constraint row under the search text box, use the drop-down menus to select the field and the operator.

   For example, **text** and **does not contain**.
3. In the text box for constraints, type the value that you want to use as a filter.

   You can list multiple values separated by comma. The operator between these values is OR.
4. (Optional) To add more constraints, click **Add Constraint**.

   A toggle button appears above the constraint rows.
5. (Optional) For multiple constraint rows, select the operator between constraints.

Option	Description
all	Select to apply the AND operation between constraint rows
any	Select to apply the OR operation between constraint rows

   By default, **all** is selected.

6 Click **Search**.

What to do next

You can save the current query to load it at a later stage.

NOTE Saved queries, dashboard charts, and alerts are not updated when you edit the field definition names that they use. If you want to apply a new field definition, you must re-create your saved query, chart, or alert.

Search Log Events by Terms

You can search for log events that contain certain alphanumeric strings.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 In the search text box, type the text or number that you are looking for and click **Search**.

Log events that contain the specified string appear in the list.

The string that you searched for is highlighted in yellow.

What to do next

You can save the current query to load it at a later stage.

Search for Events that Occurred Before and After an Event

You can search the list of log events for events that occurred before and after an event in the list.

If you want to know more about the status of your environment before and after an event, you can check the surrounding events.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, locate the event in the list.

2 At the right of the event row, click the **Set time range from this event** icon 🕓.

3 In the Set Time Range From Event dialog box, use the drop-down menus to select the period and direction of the time range.

You can select from a list of predefined periods from 1 second to 10 minutes.

4 Click **Set Range**.

The events that surround the selected event appear in the list.

NOTE This operation clears all search parameters and constraints that you have specified previously.

Clear All Filtering Rules

You can clear filtering and search results to view the list of all log events.

After you perform a search on the events list, the search results remain on the screen until you clear all queries.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, remove all constraints.

2 If text appears in the search text box, delete it.

3 Click **Search**.

Examples of Search Queries

You can use these examples when building your queries on the **Interactive Analytics** tab of Log Insight.

NOTE Some fields might not exist in the fields drop-down menu by default. You can extract fields from log events to add them to drop-down menus.

Example: Search for HTTP GET Requests that Have HTTP Status 300 or Above

To search for HTTP GET requests that have HTTP status 300 or above:

1 In the search text box, type `get`.

2 Define the constraint.

   a Select **http_status** from the field drop-down menu.

   b Select **>=** from the operator drop-down menu.

   c Type `300` in the value text box.

3 Click **Search**.

Example: Search for Requests that Come from an IP Addresses Starting with 192.168.0 and Use Internet Explorer

To search for requests from Internet Explorer that come from IP addresses starting with 192.168.0:

1 Leave the search text box empty.

2 Define the first constraint.

   a Select **browser_name** from the field drop-down menu.

   b Select **equals** from the operator drop-down menu.

   c Type `MSIE` in the value text box.

3 Click **Add Constraint**.

4 Define the second constraint.

   a Select **client** from the field drop-down menu.

   b Select **starts with** from the operator drop-down menu.

   c Type **192.168.0** in the value text box.

5 Click **Search**.

Example: Get all Log Events from January 26 to January 28 from runtime.log and runtime2.log

To search for all log events from January 26 to January 28 from the `runtime.log` and `runtime2.log` file :

1 Leave the search text box empty.

2 In the Time Range pane, use the time pickers to set the start and end date.

3 Define the constraint.

   a Select **source** from the field drop-down menu.

   b Select **equals** from the operator drop-down menu.

   c Type **runtime.log, runtime2.log** in the value text box.

4 Click **Search**.

Example: Show Events that Contain PHP URLs

To search for events that contain PHP URLs:

1 In the search text box, type **http://example.com/*.php**.

2 Click **Search**.

Using the Interactive Analytics Chart to Analyse Logs

The chart at the top of the **Interactive Analytics** tab allows you to perform analysis on the results of your query.

You can use the drop-down menus under the chart to change the chart type.

You can use the first drop-down menu to the left to control the aggregation level of the chart. The **Count** function is selected by default.

Log Insight provides several aggregation functions.

Type	Field	Description
Count	Events only	Creates a chart of the number of events for a specific query.
Minimum	Numeric fields only	Creates a chart of the minimum value for a field.
Maximum	Numeric fields only	Creates a chart of the maximum value for a field.
Average	Numeric fields only	Creates a chart of the average value for a field.
Standard Deviation	Numeric fields only	Creates a chart of the standard deviation for a field’s values.
Sum	Numeric fields only	Creates a chart of the sum of values for a field.
Variance	Numeric fields only	Creates a chart of the variance for the values of a field.

You can use the second and the third drop-down menus under the chart to group query results by specific field values rather than just as a time series.

To see the number of events for a field, for example, the number of events per host, deselect the **Time series** check box and select the check box for that field.

To see a stacked bar chart with groupings over time, select both the **Time series** check box and the field's check box.

Change the Type of the Interactive Analytics Chart

You can change the aggregation and grouping of query results displayed in the chart to graphically analyse log events.

The number of drop-down menus that you see under the chart depends on the selected aggregation function.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 Use the drop-down menus under the Interactive Analytics chart to change the aggregation function and grouping type.

- To view the number of events over time, select the **Time series** check box.
- To view only event values, deselect the **Time series** check box.

2 Click **Update**.

Example: Aggregation and Grouping in the Interactive Analytics Chart

The following table contains examples to illustrate aggregation and grouping in Log Insight charts.

Table 1-3. Example Aggregation and Grouping in the Interactive Analytics Chart

Selection in the First Drop-Down Menu	Selection in the Second Drop-Down Menu	Selection in the Third Drop-Down Menu	Text Displayed on the Screen	Result
Count	**Time series**	N/A	**Count** of events **over time**	The chart displays the number of events for the current query over time.
Average	**opLatency (vSphere)**	**Time series**	**Average** of **opLatency (vSphere) over time**	The chart displays average value of operations latency over time.
Count	**https_status** NOTE The https_status field does not appear by default. You must extract the https_status field and save the query so that https_status appears in the drop-down menu.	N/A	**Count** of events **grouped by https_status**	The chart displays the number of events for each HTTP status value.
Count	**Time series**, **https_status**	N/A	**Count** of events **over time grouped by https_status**	The chart displays HTTP status breakdown over time.

Dynamic Field Extraction

In a large environment with numerous log events, you cannot always locate the data fields that are important to you.

Log Insight provides runtime field extraction to address this problem. You can extract any field dynamically from the data by providing a regular expression. See "Examples of Regular Expressions," on page 20.

NOTE Generic queries might be very slow. For example, if you try to extract a field by using the `\(\d+\)` expression, the query returns all log events that contain numbers in parenthesis. Verify that your queries contain as much textual context as possible. For example, a better field extraction query would be `Event for vm\(\d+\)`.

You can use the extracted fields to search and filter the list of log events, or to aggregate events in the Interactive Analytics chart.

NOTE Saved queries, dashboard charts, and alerts are not updated when you edit the field definition names that they use. If you want to apply a new field definition, you must re-create your saved query, chart, or alert.

Extract Fields by Using One-Click Extract

Instead of typing context values for dynamic fields extraction, you can use the one-click extract function.

The one-click extract populates automatically all context values that correspond to the field that you select in a log event.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 In the list of log events, highlight some text in an event.

An **Extract Field** button appears next to the set of field names present in that event.

3 Click **Extract Field**.

The context values in the Fields pane are populated automatically with the context needed to extract the field that you highlighted.

4 (Optional) Adjust the Value regular expression in the Fields pane.

5 (Optional) Adjust the Context regular expression in the Fields pane.

6 Click **Test** to verify that the query returns the expected results.

The extracted field is highlighted in dark green in the list of log events. The context is highlighted in light green.

7 Select which users can access the field and click **Save**.

Option	Description
All users	All users will see the field in the search drop-down menu.
Me only	Other users will not see the field in the **Search** drop-down menu.

What to do next

You can use the extracted field to search and filter the list of log events, or to aggregate events in the Interactive Analytics chart.

You can edit saved field definitions or delete them if you no longer need them.

Note Saved queries, dashboard charts, and alerts are not updated when you edit the field definition names that they use. If you want to apply a new field definition, you must re-create your saved query, chart, or alert.

Extract Fields from Log Events

You can extract fields from log events and use these fields to search, filter, and aggregate log events.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 In the Fields pane, click **Extract Field**.

A new widget opens for you to set the parameters of the query.

3 From the drop-down menu, select a value type.

You can type a custom regular expression that matches the value of the field that you want to extract.

4 (Optional) Provide a context for the value to be extracted.

A context helps eliminate false matches, as it filters out values that do not match the provided prefix and suffix values. You can provide context values as plain text or as a regular expression.

5 (Optional) Type a name for the extracted field.

If you do not provide a name, Log Insight automatically assigns a name to the extracted field.

6 Click **Test** to verify that the query returns the expected results.

The extracted field is highlighted in dark green in the list of log events. The context is highlighted in light green.

7 Select which users can access the field and click **Save**.

Option	Description
All users	All users will see the field in the search drop-down menu.
Me only	Other users will not see the field in the **Search** drop-down menu.

Example: Example Queries for Field Extraction

You can run these queries on log events that come from a vSphere environment.

Table 1-4. Field Extraction Queries

Field to Extract	Value Type	Value	Context Before Value	Context After Value
Time taken to perform an operation	Integer	-?\d+	took	ms
HTTP version	Decimal	-?\d*\.?\d+	HTTP/	

What to do next

You can use the extracted field to search and filter the list of log events, or to aggregate events in the Interactive Analytics chart.

You can edit saved field definitions or delete them if you no longer need them.

Note Saved queries, dashboard charts, and alerts are not updated when you edit the field definition names that they use. If you want to apply a new field definition, you must re-create your saved query, chart, or alert.

Examples of Regular Expressions

You can type regular expressions in text boxes for field values to extract fields from log events.

Table 1-5. Examples of Regular Expressions

Regular Expression	Description
[xyz]	x, y, or z
(info|warn|error)	info, warn, or error
[a-z]	A lowercase letter
[^a-z]	Not a lowercase letter
[a-z]+	One or more lowercase letters
[a-z]*	Zero or more lowercase letters
[a-z]?	Zero or one lowercase letter
[a-z] {3}	Exactly three lowercase letters
[\d]	A digit
\d+$	One or more digits followed by end of message
[0-5]	A number from 0 to 5
\w	A word character (letter, digit, or underscore)
\s	White space
\S	Any character except white space
[a-zA-Z0-9]+	One or more alpha numeric characters
([a-z] {2,} [0-9] {3,5})	Two or more letters followed by three to five numbers

Note Log Insight does not support extended regex syntax.

Managing Search Queries

You can save, delete, rename, and load existing queries, export query results, and share your queries with other users.

Save a Query in Log Insight

You can save your current query and time range in Log Insight to view it later.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, perform the query that you want to save.

2 From the drop-down menu next to the **Search** button, select **Save Current Query**.

3 Type a name and click **Save**.

> **NOTE** Saved queries include a fixed time range and are not updated. By saving a query, you take a snapshot of log messages available within the time range at the moment when you save.

The query is added to the My Saved Queries list.

All users, including administrators, have an individual list of saved queries.

Rename a Query in Log Insight

You can change the name of a query that you saved in Log Insight.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 From the drop-down menu on the right of the **Search** button, select **Load Query**.

3 Point to the query that you want to rename, and click the **Edit this saved query** icon ✏.

4 Type a new name and click **Save**.

Load a Query in Log Insight

You can load queries from content packs or queries that you saved to view them on the **Interactive Analytics** tab.

Saved queries are separate from dashboard items. They do not appear on any custom dashboard. If you want to view a saved query, you have to load it.

All users, including administrators, have an individual list of saved queries.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1. From the drop-down menu on the right of the **Search** button, select **Load Query**.
2. In the Saved Queries list, click the query that you want to view on the **Interactive Analytics** tab.

   The query is loaded on the **Interactive Analytics** tab. The time range of the query is displayed above the list of events.

What to do next

You can add the query a the dashboard, change the granularity of the chart, or apply additional filtering to the query results.

Delete a Query from Log Insight

You can delete unnecessary queries from Log Insight.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1. From the drop-down menu on the right of the **Search** button, select **Load Query**.
2. Click the **Delete this saved query** icon ❌.
3. Click **Delete** to confirm.

Share the Current Query

You can send your peers a link to the current query.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1. On the **Interactive Analytics** tab, perform the query that you want to share.
2. From the drop-down menu next to the **Search** button, select **Share Current Query**.

   Log Insight displays the URL to the query.
3. Copy the URL and send it to the person that you want to share with.

Export the Current Query

You can export the results of a log query to share them with other systems, or forward them to your support contact.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1. On the **Interactive Analytics** tab, perform the query that you want to export.
2. From the drop-down menu next to the **Search** button, select **Export Query Results**.
3. Select the format and location to save the query to, and click **Save**.

Option	Description
Raw Events	Select to save the results in TXT format
JSON	Select to save the results in JSON format
XML	Select to save the results in XML format

Alert Queries in Log Insight

You can configure Log Insight to run specific queries at scheduled intervals.

If the number of events that match the query exceeds the thresholds that you have set, Log Insight can send email notifications and trigger notification events in vCenter Operations Manager.

Types of Alerts in Log Insight

You can control the intervals to run alert queries and the conditions when Log Insight sends alert notifications by selecting one of the alert types.

Alert for Any Match

The alert query is run automatically every 5 minutes. A notification is triggered when at least one event within the last 5 minutes matches the query.

Alert Based on Number of Events Within a Custom Period of Time

Alert query intervals depend on your settings. A notification is triggered according to your settings, when more or less than *X* matching events in the last *Y* minutes occurred .

If this type of alert is triggered, it is snoozed for the duration of its time period to prevent duplicate alerts from being raised for the same set of events. If you want to enable an alert while it is snoozing, you can disable and then reenable it.

Alert Based on Chart Values

The alert query triggers a notification if at least one bar in the chart is above or below the threshold that you have set, within the period that you specified.

This alert type can be set for charts that do not visualize **Count** of events **over time**.

NOTE Alert queries are user specific. Users can manage only their own alerts.

- Add an Alert Query in Log Insight to Send Email Notifications on page 24

  You can configure alert queries in Log Insight to send email notifications when specific data appears in the logs.

- Add an Alert Query in Log Insight to Send Notification Events to vCenter Operations Manager on page 25

  You can configure alert queries in Log Insight to send notification events to vCenter Operations Manager when specific data appears in the logs.

- View Existing Alert Queries on page 26

  You can view the alert queries that you have created and check whether the notifications for these queries are enabled.

- Modify an Alert Query on page 27

  You can change the trigger of a saved alert query, and enable or disable the notifications that the query sends.

- Delete an Alert Query on page 27

  You can delete alert queries when you no longer need them.

Add an Alert Query in Log Insight to Send Email Notifications

You can configure alert queries in Log Insight to send email notifications when specific data appears in the logs.

Prerequisites

- Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1. On the **Interactive Analytics** tab, run the query for which you want notifications to be sent .
2. From the drop-down menu on the right of the **Search** button, select **Add Alert** .
3. In the Add Alert dialog box, type a name for the alert, and provide a short meaningful description of the event that triggers the alert.

   The alert name and description are included in the email that Log Insight sends.
4. Select the **Email** check-box and type the email address where Log Insight will send the notifications.

   Use commas to separate multiple addresses.
5. Set the alert type.

Alert Type	Selection
Any Match	Select the **on any match** option. Queries run every 5 minutes.
Based on number of events within a period of time	Select the second radio button and use the drop-down menus to set the parameters. Queries run based on your settings.
Based on chart values	Select the third radio button and use the drop-down menus to configure the parameters. NOTE You cannot assign alert queries to charts that visualize **Count** of events **over time**.

   The orange line in the preview chart shows the current threshold.
6. Click **Save**.

What to do next

You can enable and disable your saved alerts, or delete them if you no longer need them.

NOTE Alert queries are user specific. Users can manage only their own alerts.

Add an Alert Query in Log Insight to Send Notification Events to vCenter Operations Manager

You can configure alert queries in Log Insight to send notification events to vCenter Operations Manager when specific data appears in the logs.

Notification events that Log Insight generates are associated with resources in vCenter Operations Manager. You can read more about resources in the *vCenter Operations Manager Getting Started Guide (Custom User Interface)*

NOTE Several minutes are required for notification events to appear in the vCenter Operations Manager user interface.

Prerequisites

- Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 On the **Interactive Analytics** tab, run the query for which you want notifications to be sent .

2 From the drop-down menu on the right of the **Search** button, select **Add Alert** .

3 In the Add Alert dialog box, type a name for the alert, and provide a short meaningful description of the event that triggers the alert.

The alert name and description are included in the notification event that Log Insight sends.

4 Select **Send to vCenter Operations Manager**.

5 Select a vCenter Operations Manager resource to be associated with the notification events that Log Insight sends.

6 Set the alert type.

Alert Type	Selection
Any Match	Select the **on any match** option. Queries run every 5 minutes.
Based on number of events within a period of time	Select the second radio button and use the drop-down menus to set the parameters. Queries run based on your settings.
Based on chart values	Select the third radio button and use the drop-down menus to configure the parameters. **NOTE** You cannot assign alert queries to charts that visualize **Count** of events **over time**.

The orange line in the preview chart shows the current threshold.

7 Click **Save**.

When the alert query returns results that trigger a notification, a notification event is sent to vCenter Operations Manager.

Notification events appear in several locations, depending on the vCenter Operations Manager user interface that you use.

Example: Configure a Notification Alert to vCenter Operations Manager

Assume that in vCenter Operations Manager you have a virtual machine resource named vm-abc with the IP address 168.0.0.5.

You have configured Log Insight to pull events from the vCenter Server system where the virtual machine vm-abc runs.

You want to receive a notification in vCenter Operations Manager each time the vm-abc virtual machine is powered off.

Here is how to configure Log Insight to send these notification events to vCenter Operations Manager.

1 In the search text box, type `Power Off virtual machine`.

2 Click **Add a Constraint**, select **source** and **equals**, and type `168.0.0.5`.

3 Click **Search**.

If the vm-abc virtual machine has been powered off during the selected time range, the search returns all instances that occurred.

4 From the drop-down menu on the right of the **Search** button, select **Add Alert**.

5 In the Add Alert dialog box, type a name and description for the alert, and select **Send to vCenter Operations Manager**.

6 Click **Select**, type `vm-abc`, and click **Search** to find the vm-abc resource in the list.

7 Click the vm-abc resource in the list to add it.

8 Under Raise an alert, select **on any match**.

9 Click **Save**.

Log Insight polls the vCenter Server system at five-minute intervals. If the query returns a new Power Off virtual machine task from source 168.0.0.5, Log Insight sends a notification event that is associated with the vm-abc resource in vCenter Operations Manager.

What to do next

You can enable and disable your saved alerts, or delete them if you no longer need them.

NOTE Alert queries are user specific. Users can manage only their own alerts.

View Existing Alert Queries

You can view the alert queries that you have created and check whether the notifications for these queries are enabled.

NOTE Alert queries are user specific. Users can manage only their own alerts.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 From the drop-down menu on the right of the **Search** button, select **Manage Alerts**.

3 View the list of your alert queries.

The status of alert notifications is displayed under the name of the query.

What to do next

You can click alert queries in the list to modify their parameters, or delete the queries that you no longer need.

Modify an Alert Query

You can change the trigger of a saved alert query, and enable or disable the notifications that the query sends.

Note Alert queries are user specific. Users can manage only their own alerts.

Prerequisites

- Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 From the drop-down menu on the right of the **Search** button, select **Manage Alerts**.

3 In the Manage Alerts list, click the alert query that you want to modify.

4 Change the parameters of the query and click **Save**.

If you deselect both notification options, the alert query is disabled.

Delete an Alert Query

You can delete alert queries when you no longer need them.

Note Alert queries are user specific. Users can manage only their own alerts.

Prerequisites

Verify that you are logged in to the Log Insight Web user interface. The URL format is https://*log_insight-host*, where *log_insight-host* is the IP address or host name of the Log Insight virtual appliance.

Procedure

1 Navigate to the **Interactive Analytics** tab.

2 From the drop-down menu on the right of the **Search** button, select **Manage Alerts**.

3 Point to the query that you want to delete and click the **Delete** icon ✖.

Index